Basic Hazard Recognition

The ability to recognize hazards is the fundamental investigative skill. It forms the basis for all other skills that an investigator will utilize. In other words, an investigator must be able to recognize that a problem exists, before any analysis for causation can help produce a countermeasure. This is true for anyone avoiding risk in fluid movement as well. Reaction time begins with recognition of a hazard or of a threat. One principle of occupational safety is "early intervention." This concept drives the management of safety. Basically, the sooner a hazard is recognized and subsequently countered, the less loss will be incurred from hazard.

It is important to have a visual model for recognizing hazards. One such model that guides hazard recognition attempts to make categories of hazard as unique as possible, identify a source of the hazard category, and then categorize the results of exposure. This technique could be used for any asset or human that was to be protected.

Let's look at a possible listing of hazard categories to human workers. The categories may be listed as: Impact, Penetration, Compression, Chemical, Respiratory, Temperature, Visibility, Radiation, Walking/Working Surface, Electricity, Animal, Insect, Vermin, Biological, Noise, and Ergonomic.

These categories will have types and many possible specific sources. Let's look at some examples in the chart below.

Category	**Type**	**Source(s)**
Impact	Struck by Object Bump/run into Object Vibration	Boom of backhoe, vehicle/traffic, train, etc. Overhanging structure, access to tight space Jackhammer use
Penetration	Sharp edges Injection Impalement	Edges of metal Hydraulic oils under pressure Uncapped rebar
Compression	Pinch Entrapment	Ingoing nip points Heavy object that pins down or restricts
Chemical	Burn Toxicity	Acid Carcinogen
Respiratory	Dust Oxygen deficient	Asbestos fiber, silica dust Displaced oxygen levels in confined spaces
Temperature	Cold Heat	Walk-in freezers, outdoor temperature Sun, ovens, chemical reactions/fire
Radiation		Sun, lighting sources, radioactive elements, x-rays
Visibility	Contrast Blocked view Distortion	Low lighting Blind spots Looking into or through substance
Walking/Working Surfaces	Slippery Trip Height	Contaminants on dry surface Uneven walkway, cords Different levels
Electricity	Shock	Amperage, Lightning

	Burn Electrocution	Heat from resistance Amperage, Lightning
Animal/Insect/Vermin	Penetration Poison	Physical penetration of teeth, fangs, stinger Toxic exposure to poison
Biological	Bacterial Viral	Staff infections Hepatitis B, C, HIV
Noise		Loud machinery Concussion/blast waves
Ergonomic	**Physica**l: Overexertion Repetitive stress/trauma Vibration **Environmental Demands** **Mental Demands**	Strains from heavy lifting/improper lifts Typing, repetitive reaching/scanning Jackhammer usage Hand high position on controls Too many audible indicators Stress

In the above chart categories are as specific as possible without much overlap. While the category may have numerous types of hazard and sources that vary widely, each category produces results. These results are either chronic or acute and at the same time, physical or health related. Acute results from exposure are immediate or appear or manifest themselves shortly after exposure. Chronic results are those that build or develop over lengthy periods. Sometimes both results happen concurrently. This is why merely classifying hazards as physical or health hazards is not preferable. Look at the following chart for specific examples.

Category	**Type**	**Result**
Penetration	Injection of hydraulic fluid from pressure	Fluid injection injury with acute physical loss of finger and hand control; chronic effect of tissue toxicity
Chemical	Skin exposure: trichloroethylene	Dry, irritation of skin as acute results Parkinson disease from chronic health exposure

Hazard recognition with a basis from hazard categories can also be a strategy for general walk through inspections and focused inspections of machinery or areas in regard to safety management topics. Rather than trying to memorize or know numerous specific violations of OSHA regulations, looking for categories of hazard, identifying the source, and then researching relevant regulations and standards, can aid the safety professional in proactive investigations or audits.

Threats

Tactical personnel are those that rely on a team formulated and consistent set of tactics or way of overcoming a threat. Typically we might view tactical personnel as police, security, special response teams, military units, firefighters, rescuers, and others that deal with threats.

A threat is not a hazard. A hazard does not involve culpability. A hazard is present or exists without intent. A person might not recognize it or interpret its presence or danger, but it is present

physically and does not change. Of course, the hazard can have potential results that change as the environment surrounding it changes. For example, an excavator that is working and rotating its superstructure close to a stationary object presents a compression hazard between the stationary object and the swinging superstructure. As long as the situation remains similar the hazard remains, regardless of whether a human realizes that the superstructure could compress him or her between the stationary object and machine.

A threat is more fluid and changes based upon human intent. In can involve a subject assaulting another, it could involve setting traps, or using hazards to cause harm. Mental culpability involves the mental intention of human action from careless action to intentional action. It is not necessarily in regard to the actions, but to the immediate results of the actions.

Culpability is the state of mind of the person in regards to intent at the time of occurrence. We generally have four levels that must be considered;

1. Reckless,
2. Wanton,
3. Knowing, and
4. Intentional.

Reckless means that the person did not recognize the chance or act could result in the outcome. This describes the worker who forgot to pull down his safety glasses right out of lunch. Wanton describes a condition where the worker should have known that the risk of his or her action or failure to take action could result in the consequences, in other words the offender takes a calculated risk. Knowing describes a condition where the worker had actual knowledge that the action or failure to act would result in the consequence. Intentional describes a condition where the offender intended to cause the consequences.

Culpability is relevant in criminal acts or acts of recognized combat as well. But it is the connection from human behaviors to their contribution to a loss incident. Because of intent and fluid changes to intent, threats are handled differently in many cases than hazards.

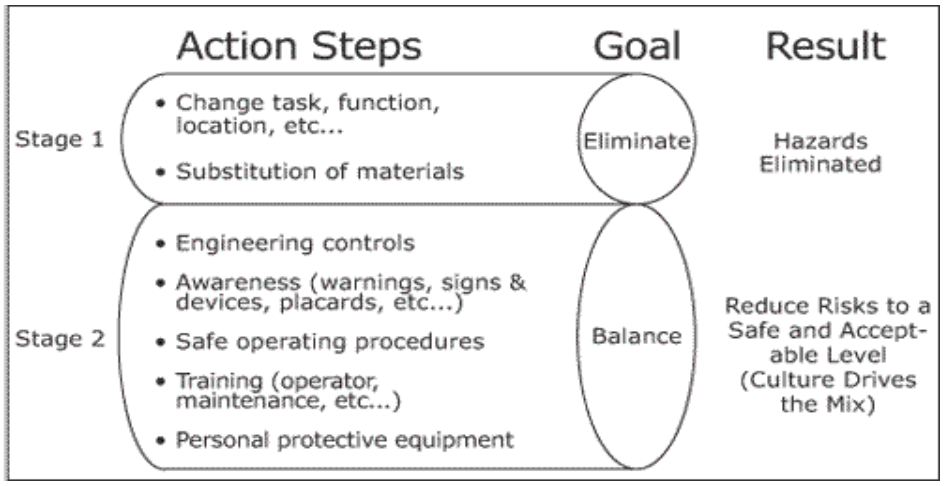
Vulnerabilities

A vulnerability is an exposure to a condition that would allow for a threat to be successful in creating a loss to that which is to be protected. It could be an unlocked door, it could be an open approach to a building, or an easily broken and accessed window. While a 100% secure asset may be a theory or goal, it comes down to balancing vulnerabilities with available resources. This is security management.

Hazard Abatement

Hazard abatement begins with causal analysis. Root cause analysis begins with principle that one cause to an incident is rare. An incident, or occurrence that had a potential for negative risk, is the result of an alignment of conditions and events. An alignment of events and conditions allows for the specific chain of events to occur. If one event or condition, or the chronological order was interrupted the incident would not have, could not have, or would certainly have changed enough not to be the same incident.

Hazards are overcome from the ANSI hazard control model shown below in figure 1.



ANSI B11-2008.

The overall strategy centers on preventing human contact with the hazard or balance or managing it with limiting contact. Effectiveness is not efficiency and efficient work is safe work because it balances risk and effectiveness.

Countering threats for tactical personnel involves accepting the concept of effectiveness being safety. In other words, when an intentional threat is encountered, the effective countering of the threat decreases the risk to the overall team. This concept does not involve avoiding as an overall strategy. For example, if a special response team is deployed to counter an active shooter, the team must engage the threat and effectively and quickly mitigate the threat.

The Strategical, Tactical, and Protective model of tactical personnel safety embraces the concept of effectiveness being directly related to safety. In other words, planning and approach to a threat involves an interwoven and matching interaction between the strategical side of planning, the tactics developed, trained, and deployed, and then the final protective measures used to protect the team as well as the individual.

Countering vulnerabilities involves matching the security measure with the goal of the level of security that it is deployed. Security has 5 levels: deter, detect, impede, respond, and rehabilitate (Philpott, 2001). Each level has its own goal. Deterrence level has the goal of deterring the decision to exploit or attempt to exploit a vulnerability. Measures deployed here may be physical or not. Detection

aims at being aware of a breach of perimeter, or boundary denoting protection. Impeding the progress of the breach allows for proper response. The quicker the detection is accomplished and the more effective the slowing of the penetration, the more time for response is allowed. Depending on the situation, the response can be matched to the overall threat. The final level is rehabilitation, which includes restoration of any barriers, clearance of the grounds, and continuous improvement to the security countermeasures based upon the performance of the overall security system.

Matching the security measures to the goals of the level deployed is critical. For examples, cameras might be deployed in all 5 stages in different manners and their use must match the goal of its deployment. Cameras used for deterrence will not be hidden and might even be warned against in attempt to increase its deterrence influence. Cameras used to detect entry are usually monitored and might even have software that detects movement or other presence to a human watch. Cameras may not slow a breach unless the perpetrator is avoiding them or attempting to disable them as they progress. Cameras deployed in the rehabilitation stage are typically aimed at gathering evidence for prosecution as well as training and security needs assessments. Security measures are more or less effective depending on how they are deployed.

The successful safety professional must have a foundational grasp of recognizing hazards, threats, and vulnerabilities as well as an understanding of abatement strategy.